nLightened Thoughts

February 2011

William Blinn Communications
Worthington, Ohio 43085
www.n-lighten.us • 614/859.9359

It's the Worst Virus Ever!!!! (from an e-mail warning)

How often do you receive a message like this? If you open a message with an attachment called "foo.mp4", your hard drive will be erased and your computer will be vaporized!!! This has been confirmed by Microsoft and Snopes and MSNBC, so I know it's true!!! Please forward this message to everyone you know!!! What do you do with a message like that? Whatever you do, please don't forward it.

Messages like this seemed to have died out, but I've noticed a resurgence that started in the fourth quarter of 2010. You might ask, *Isn't a bogus warning better than a computer virus?* That's the wrong question. It's like asking whether being gored by a wild boar is better than a collision with a transit bus. There's no relationship.

Bogus warnings that are forwarded indiscriminately are bonanzas for fraudsters. Because people are people, a certain number of mistakes will lead to the compromise of some number of computers. Compromised computers will yield e-mail addresses and a message that has been forwarded many times has almost certainly collected dozens, if not hundreds, of e-mail addresses. So besides needlessly raising the fear level among computer users, these fake alarms actually play into the hands of the bad guys.

I learned not to open unexpected attachments early when I fell for the first mass-distributed computer worm (ILOVEYOU, May 4, 2000). Although my computer was on a LAN, I recognized the problem and disconnected the network cable fast enough that the infection was limited to my computer. Even then I should have known better and I've never been victimized in the nearly 11 years since even though I've received plenty of messages that contained infected attachments.

A good antivirus application and Postini inspection ahead of my computer's e-mail in-box have reduced the number of virus-laden messages that reach my computer to near zero but even if these protections had been absent, there has been no threat in the past 11 years that would have infected my computer. Protecting yourself and your computer isn't a question of being a high-tech genius; all it requires is a bit of common sense and logic.

Most messages with links to phishing sites, worm or virus attachments, or other threats might as well have Don't Open Me in 96-point red type, highlighted in yellow. They are that obvious most of the time and that's what makes the phony warnings so annoying.

Tell-Tale Signs

Fraudulent (phishing) messages have certain characteristics that make them easy to spot.

- If the message is "from" you, delete it unless you've sent a message to yourself.
- Don't depend on the "from" address. It's easy for anyone who has just a tiny bit of technological know-how to create a message that appears to have come from anyone.
- Don't depend on the presence of corporate graphics. Just because the message contains a Bank of America logo or a PayPal logo doesn't mean that's where the message came from.
- If a message threatens loss of account privileges or says that you made a purchase that you didn't make, it is probably a hoax. If you're uncertain, use your telephone to contact the financial institution, Internet service provider, or store. Do not use any link on the e-mail or any phone number provided by the e-mail.
- If the message asks you to "confirm" any information that the store or financial institution should already have, the message is phony. No bank will ever send a message that asks you to fill out a form that confirms your account number, security question, social security number, address, phone number or PIN. Period.
- If the message claims that you ordered something but provides a link that you can click just in case you didn't really place the order and want to cancel it, the message is a clearly bait.

But rather than trying to think of all the possible indications that a message is bad, it's easier to look for clear indications that the message is valid.

nLightened Thoughts (ISSN 1543-1533) is for clients and friends of n-Lighten.us, 179 Caren Avenue, Worthington, Ohio 43085. Phone 614.859.9359. On the Web at www.n-Lighten.us.

When you receive a message with either a link that the sender asks you to follow or an attachment the sender wants you to open, ask yourself a few questions.

Message Checklist

The following list of questions may appear intimidating but you can perform most of the tests in about the same amount of time it takes to look both ways before crossing a street. In other words, it takes far longer to explain the tests than it does to actually do the tests.

- Is this message from someone I know? (If yes, proceed.)
- Is this message from someone who routinely sends me messages? (If yes, proceed.) If you are an entry-level employee, the CEO may not be in the habit of sending messages that are personally addressed to you.
- Does the message read the way a message from the sender would read? (If the message seems to be in character, proceed.) If the sender is someone who has an advanced degree and who is generally careful about spelling and punctuation, *Hay, dood, this is 4U* may indicate that the message is from someone else.
- Am I expecting a message with an attachment or a link from this sender? Did I ask the sender for a copy of a business proposal? Does the sender usually send me links to websites? (If so, proceed.)

For Links

- Is there an explanation of what the link is?
- Does the link go where it claims to go? Hovering the mouse over the link will display, somewhere on the screen, the actual link target.
- Does the link make sense? A link to "www.heave.to/support.harvard.edu" will not take you to Harvard University; instead, it will take you to "heave.to" and open a file in a directory named "support.harvard.edu".
- Is the target site safe? Well known sites (Microsoft, Google, Yahoo, and the like) are generally safe. If you know a site (techbyter.com, for example), you can reasonably consider it to be safe. If it's a domain you've never heard of, it doesn't hurt to perform a Google search to see what others have to say about it.
- If you have any concern about the link, contact the sender to ask about it.

For attached files

- Is this the kind of file I would expect from the sender? Is it named appropriately? An MP4 file from somebody who has never sent you an MP4 file would be suspicious.
- Some e-mail applications allow you to open a file by double-clicking it. Instead, save the file to your computer and run a virus scan on it.
- A test by an antivirus program isn't conclusive. A false result simply means that the test didn't find anything; somebody has to be the first one to encounter a new threat and it might be you.

If anything has raised any concerns, contact the sender before you do anything with the file and if you value the files on your computer, never implicitly trust any e-mail message. Ω

Social Networking? Bah! That's for Lazy Children!

If that's your opinion of LinkedIn, Plaxo, or even Facebook and Twitter, you could be missing a lot of good opportunities.

Twitter, for example, has the reputation of being a service that's used by people who have nothing better to do than post messages about eating peanut butter sandwiches. Not so! I don't use Twitter as much as I should, but I do occasionally *tweet*. And I know several people who actively use the service to find new clients.

Facebook is more about personal connections than business connections, but it's fun to find family members that you usually communicate with once or twice a year and start an ongoing conversation. Likewise people you knew in high school or college.

For business people a service such as Plaxo or LinkedIn is about as important as your e-mail address.

I've had a LinkedIn account for several years but hadn't been actively using it for anything. When I had some free time around the end of 2010, I started looking to see what was available from the service.

In addition to finding and reconnecting with people I worked with 15 years ago and more, I found groups for people who work in various industries (such as manufacturing), who have certain job functions (auditing), who live in a specific city (Denver), or who are interested in just about any topic (electronic book readers).

An auditor who works for Honda in Marysville would probably be the only large-company auditor living in the area. Using LinkedIn, the auditor could easily talk with others in similar positions from Columbus and New York to Chicago, London, Paris, and Moscow.

At the other end of the scale, city-based groups allow everyone who lives in a geographic area to discuss local issues at times and locations that are convenient. All members of a group that wants to improve the neighborhood don't have to set aside Thursday evening at 6:30 for a meeting; the discussion happens over several days online.

Any intelligent business person knows that networking is important to success but most of us simply don't have time to set aside for networking meetings.

Social networking can help! Ω